Oracle Banking Digital Experience

Core Help Desk User Manual
Release 15.1.0.0.0

Part No. E66313-01

October 2015

ORACLE®

Core Help Desk User Manual

October 2015

Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway

Goregaon (East)

Mumbai, Maharashtra 400 063

India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax: +91 22 6718 3001

www.oracle.com/financialservices/

Copyright © 2008, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

1. Preface 4
2. Transaction Host Integration Matrix 5
3. Introduction 6
4. Advance Search 7
5. Manage Policies 12

1. Preface

1.1 Intended Audience

This document is intended for the following audience:

- Customers
- Partners

1.2 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

1.3 Access to OFSS Support

https://support.us.oracle.com

1.4 Structure

This manual is organized into the following categories:

Preface gives information on the intended audience. It also describes the overall structure of the User Manual.

Transaction Host Integration Matrix provides information on host integration requirements for the transactions covered in the User Manual.

Introduction provides brief information on the overall functionality covered in the User Manual.

The subsequent chapters provide information on transactions covered in the User Manual.

Each transaction is explained in the following manner:

- Introduction to the transaction
- Screenshots of the transaction

The images of screens used in this user manual are for illustrative purpose only, to provide improved understanding of the functionality; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.

- Procedure containing steps to complete the transaction- The mandatory and conditional fields of the transaction are explained in the procedure.

If a transaction contains multiple procedures, each procedure is explained. If some functionality is present in many transactions, this functionality is explained separately.

1.5 Related Information Sources

For more information on Oracle Banking Digital Experience Release 15.1.0.0.0, refer to the following documents:

Oracle Banking Digital Experience Licensing Guide

2. Transaction Host Integration Matrix

Legends

NH	No Host Interface Required
★	Host Interface to be developed separately
✓	Pre integrated Host interface available
✕	Pre integrated Host interface not available

Transaction Name	FLEXCUBE UBS	Third Party Host System
Advance Search	NH	NH

3. Introduction

Using the *Help Desk User* module the *Bank Administrator* carries out various transactions required on behalf of the customer. The transactions available for the *Help Desk User* are mainly for advance search and view purpose.

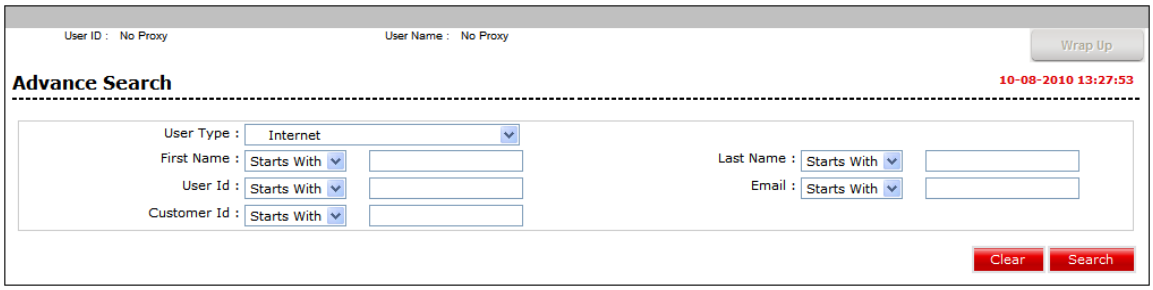
4. Advance Search

Using the **Advance Search** option the Help Desk User can carry out an advanced search to view the user details and login in the application on behalf of the selected use.

To search a record

1. From the drop-down list, select the appropriate search criteria.
2. In the adjacent field, enter the search criteria.

Advance Search



Field Description

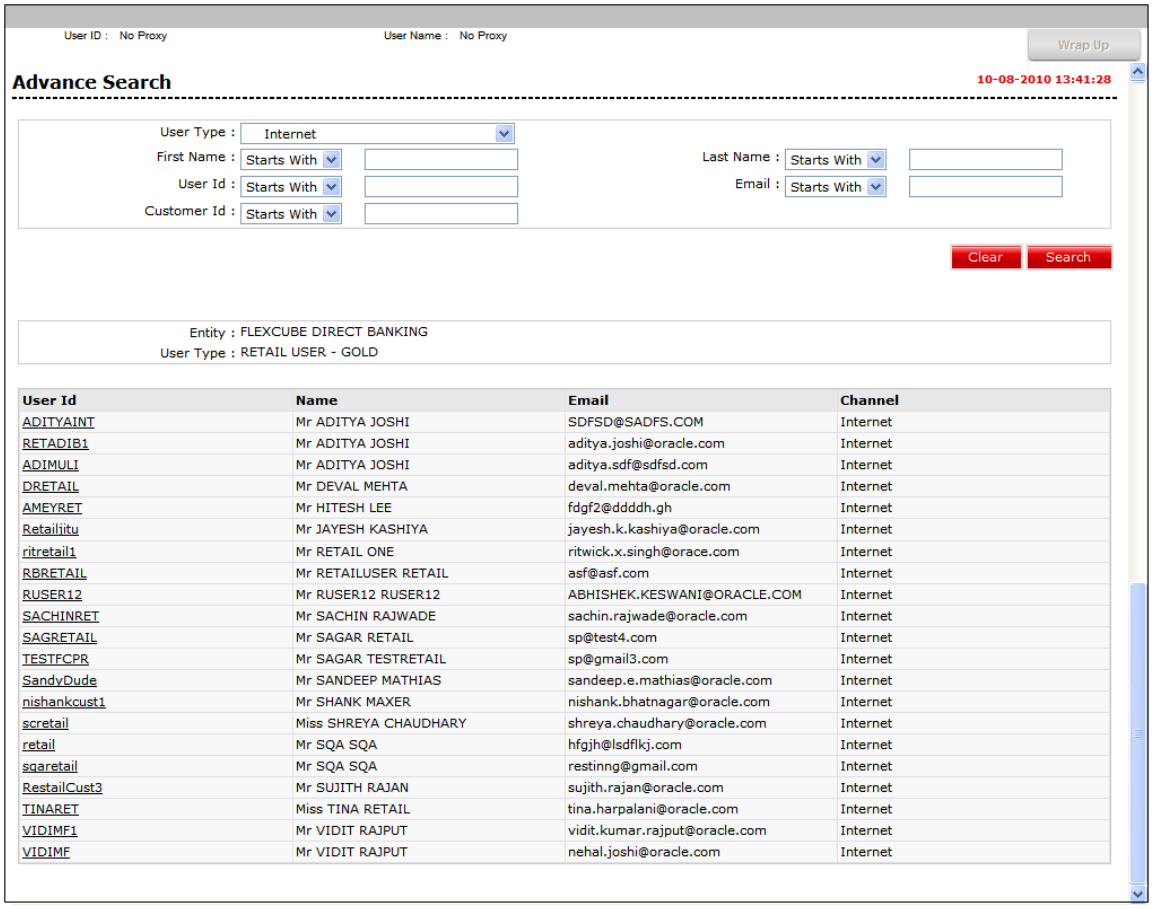
Field Name	Description
User Type	[Mandatory, Drop-Down] Indicates the user type.
First Name	[Optional, Drop Down, Alphanumeric, 40] Indicates the first name of the customer. The options are: • Starts with • Ends with • Equals • Contains The *Search* clause helps in enhancing the search criteria by indicating the position of the characters entered in the adjacent field. **For Example:** If you select the search criteria as **Starts With** and enter **A** in the adjacent field, then the system displays all the customers' first names starting with **A**.

Field Name	Description
Last Name	[Optional, Drop Down, Alphanumeric,40] Indicates the last name. The options are: • Starts with • Ends with • Equals • Contains The *Search* clause helps in enhancing the search criteria by indicating the position of the characters entered in the adjacent field. **For Example:** If you select the search criteria as **Starts With** and enter **E** in the adjacent field, then the system displays all the customers' last names starting with **E.**
User ID	[Optional, Drop Down, Alphanumeric,18] Indicates the user ID. The options are: • Starts with • Ends with • Equals • Contains The *Search* clause helps in enhancing the search criteria by indicating the position of the characters entered in the adjacent field. Type the *Search* string in the adjacent field. **For Example:** If you select the search criteria as **Starts With** and enter **1** in the adjacent field, then the system displays the entire user IDs starting with **1.**

Field Name	Description
Email	[Optional, Drop Down, Alphanumeric,18] Indicates the email. The options are: • Starts with • Ends with • Equals • Contains The *Search* clause helps in enhancing the search criteria by indicating the position of the characters entered in the adjacent field. Type the search string in the adjacent field. **For Example:** If you select the *Search* criteria as **Starts With** and enter **L** in the adjacent field, then the system displays all the email IDs starting with **L.**
Customer Id	[Optional, Drop Down, Alphanumeric,20] Indicates the customer ID. The options are: • Starts with • Ends with • Equals • Contains The *Search* clause helps in enhancing the search criteria by indicating the position of the characters entered in the adjacent field. Indicates the search string. **For Example:** If you select the *Search* criteria as **Starts With** and enter **1** in the adjacent field, then the system displays all the users whose customer ID starts with **1.**

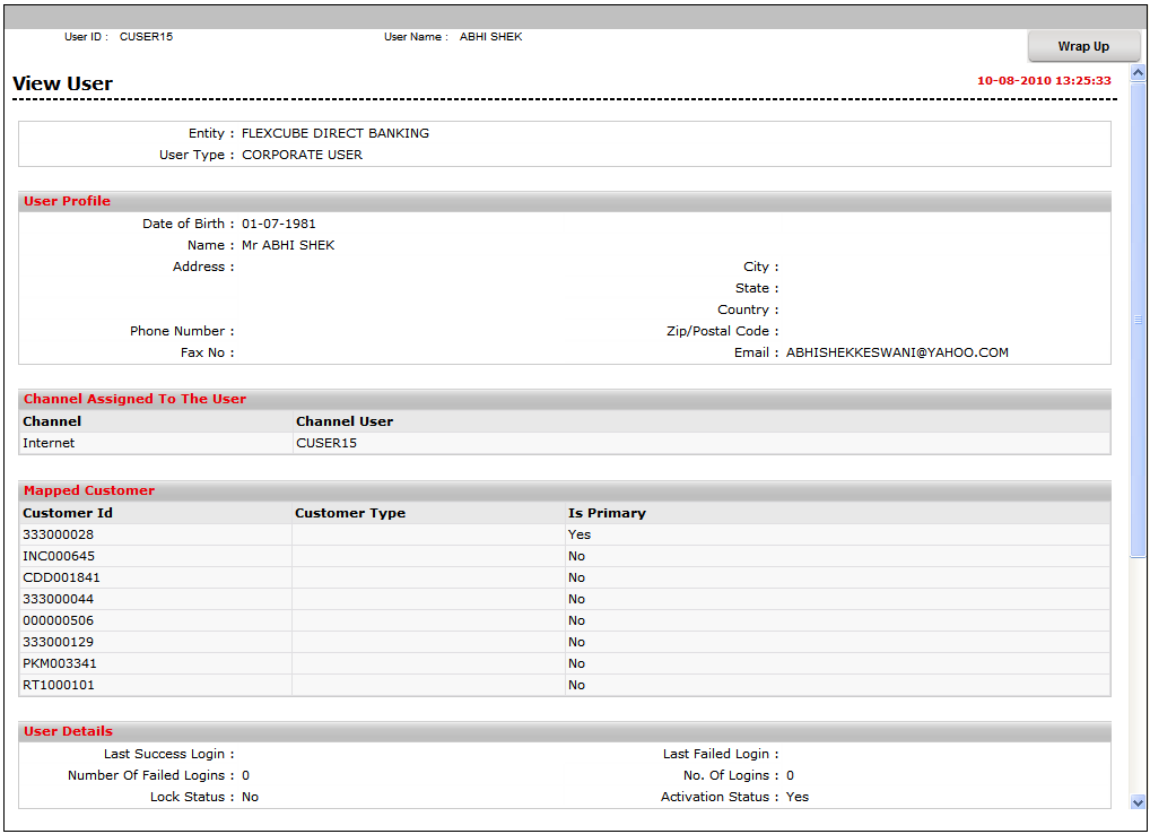
3. Click **Search**.
The **Advance Search** screen with the search result appears.

Advance Search



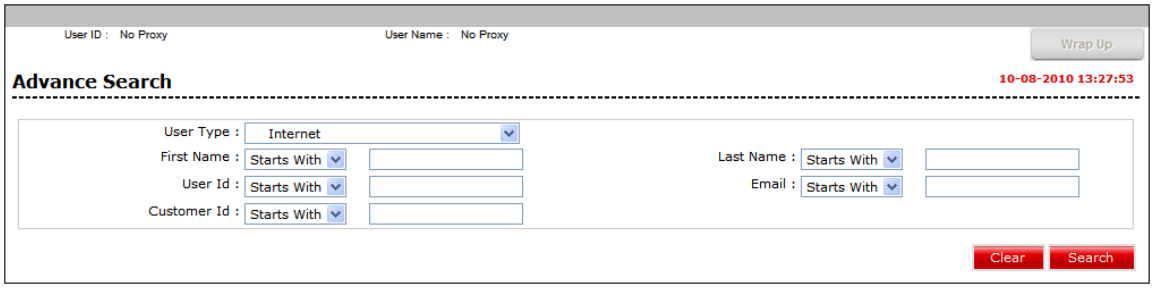
4. Click the link under **User Id**.
The **View User** screen appears.

View User



5. Click **Wrap Up.**
The **Advance Search** screen appears.

Advance Search



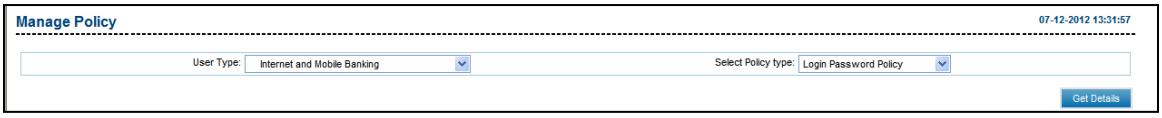
5. Manage Policies

The *Bank Administrator* can set *User ID and Password Policy* for different user types for available channels. The parameters can be set-up at each entity. The *Manage Policy* option allows the *Bank Administrator* to select the *User Type* and *Type of Policy* which is to be set up.

To set a password policy

1. From the **Maintenance** menu, select **Manage Policy**.
   The **Manage Policy** screen appears.

Manage Policy

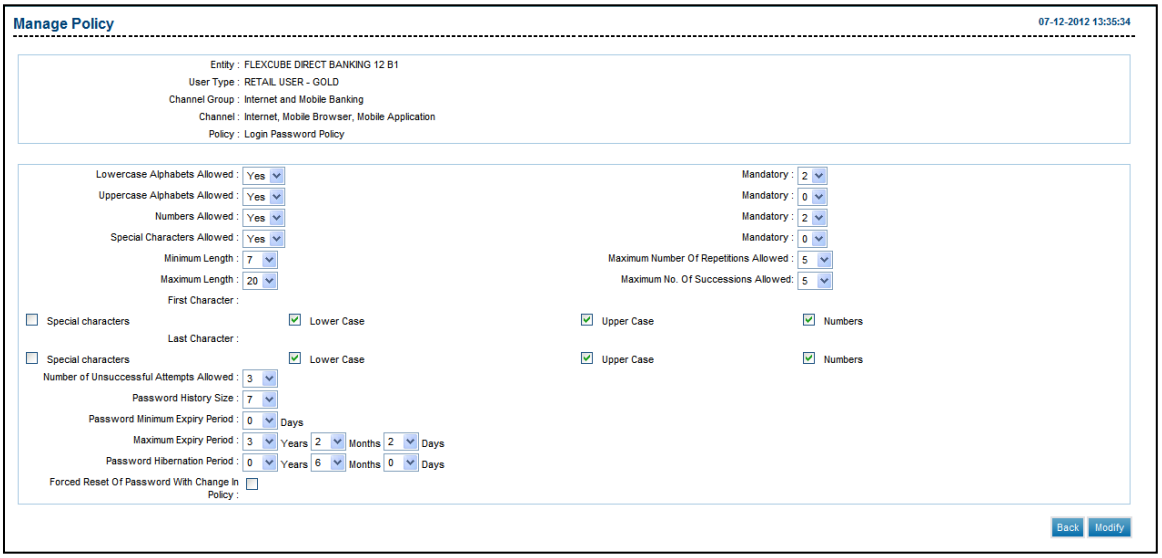


Field Description

Field Name	Description
User Type	[Mandatory, Drop-Down] Indicates the user type.
Select Policy Type	[Mandatory, Drop-Down] Indicates the policy type. The options are: • Login Password Policy • Transaction Password Policy • User ID Policy

2. Select the User Type and Login Password Policy from the drop-down list.
3. Click **Get Details**.
   The **Manage Policy** screen appears.

Manage Policy – Login Password Policy



4. Select the appropriate Password Policy details. Here details are shown for the Login Password Policy.

Manage Policy – User ID Policy

Field Description

Field Name	Description
Entity	[Display] Displays the entity name.
User Type	[Display] Displays the user type.
Channel Group	[Display] Displays the channel group for which the policy is being set.
Channel	[Display] Displays the channel for which the policy is being set.

Field Name	Description
Policy	[Display] Displays the password policy set to the user type.
Lowercase Alphabets Allowed	[Mandatory, Drop-Down] Indicates whether the lowercase alphabets are allowed in a password. The options are: • No • Yes
Mandatory	[Conditional, Drop-Down] Indicates the number of lowercase characters allowed in a password. The options are: • 0 • 1 • 2 • 3 • 4 • 5
Uppercase Alphabets Allowed	[Mandatory, Drop-Down] Indicates whether uppercase alphabets are allowed in a password. The options are: • No • Yes

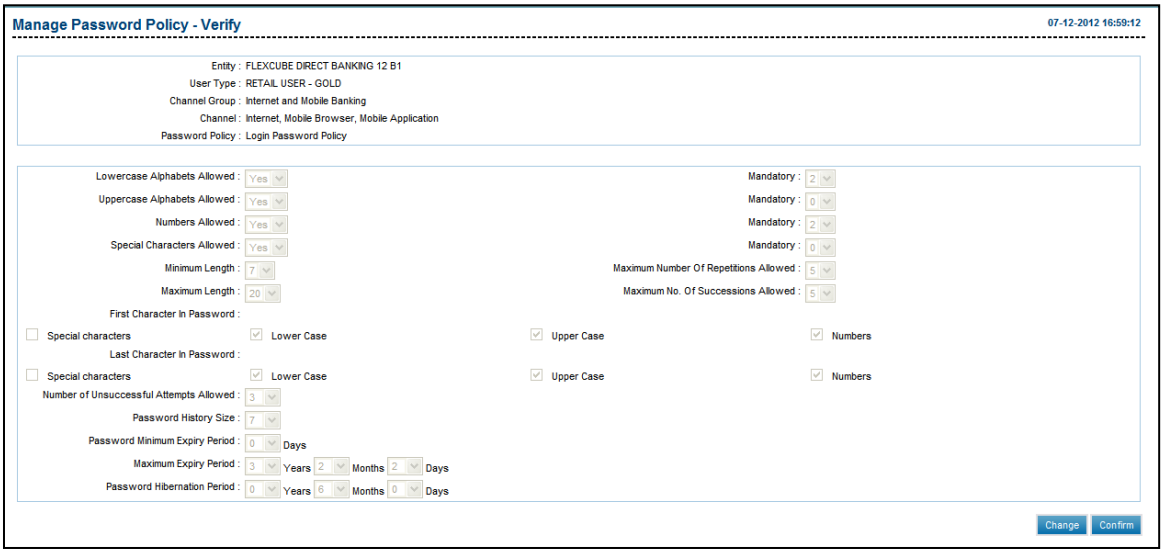
Field Name	Description
Mandatory	[Conditional, Drop-Down] Indicates the number of uppercase characters allowed in a password. To enable this field, select the **Yes** option, from the **Uppercase Alphabets Allowed** list. The options are: • 0 • 1 • 2 • 3 • 4 • 5
Numbers Allowed	[Mandatory, Drop-Down] Indicates whether numeric values are in the password. The options are: • No • Yes
Mandatory	[Conditional, Drop-Down] Indicates the number of numeric characters allowed in a password. To enable this field, select **Yes** option, from the **Numbers Allowed** list. The options are: • 0 • 1 • 2 • 3 • 4 • 5
Special Characters Allowed	[Mandatory, Drop-Down] Indicates whether special characters are allowed in the password. The options are: • No • Yes

Field Name	Description
Mandatory	[Conditional, Drop-Down] Indicates the number of special characters allowed in a password. To enable this field, select **Yes** option, from the **Numbers Allowed** list.
Minimum Length	[Mandatory, Drop-Down] Indicates the minimum password length. The options are: • 4 • 5 • 6 • 7 • 8 • 9 • 10
Maximum No. of Repetitions Allowed	[Mandatory, Drop-Down] Indicates the maximum number of repetitions allowed. The options are: [0-20]
Maximum Length	[Mandatory, Drop-Down] Indicates the maximum password length.
Maximum No. Of Successions Allowed	[Mandatory, Drop-Down] Indicates the number of successful attempts allowed to enter a password.
First Character In Password	[Mandatory, Check Box] Indicates first allowed character in password. The options are: • **Special Character**: Indicates whether first character in password should be a special character. • **Lower Case**: Indicates whether the first character is allowed as lower case. • **Upper Case**: Indicates whether the first character is allowed as upper case in the password. • **Numbers**: Indicates whether the first character is allowed as numeric characters.

Field Name	Description
Last Character In Password	[Mandatory, Check Box] Indicates the last allowed character in the password. The options are: • **Special Character**: Indicates whether the last character in password should be a special character. • **Lower Case**: Indicates whether last character is allowed as lower case. • **Upper Case**: Indicates whether the last character is allowed as upper case in the password. • **Numbers**: Indicates whether the last character is allowed as numeric characters.
Number of Unsuccessful Attempts Allowed	[Mandatory, Drop-Down] Indicates the number of unsuccessful attempts allowed. The account will be locked after the specified number of attempts. This field is applicable for password policy.
Password History Size	[Mandatory, Drop-Down] Indicates the password history. The system retains a log of old passwords which cannot be repeated. This field is applicable for password policy.
Password Minimum Expiry Period	[Mandatory, Drop-Down] Indicates the password minimum expiry period. This field is applicable for password policy.
Maximum Expiry Period	[Mandatory, Drop-Down] Indicates the password maximum expiry period in years. The options are: • Years - [0-10] • Months - [0-11] • Days - [0-30] The period set cannot be less than the minimum password expiry period.
Password Hibernation Period	[Mandatory, Drop-Down] Indicates the password hibernation period. This field will be enabled only for *Password Policy*.
Forced Reset Of Password With Change In Policy	[Mandatory, Check Box] Indicates whether forced reset of password with change in policy is available. This field will be enabled only for password policy.

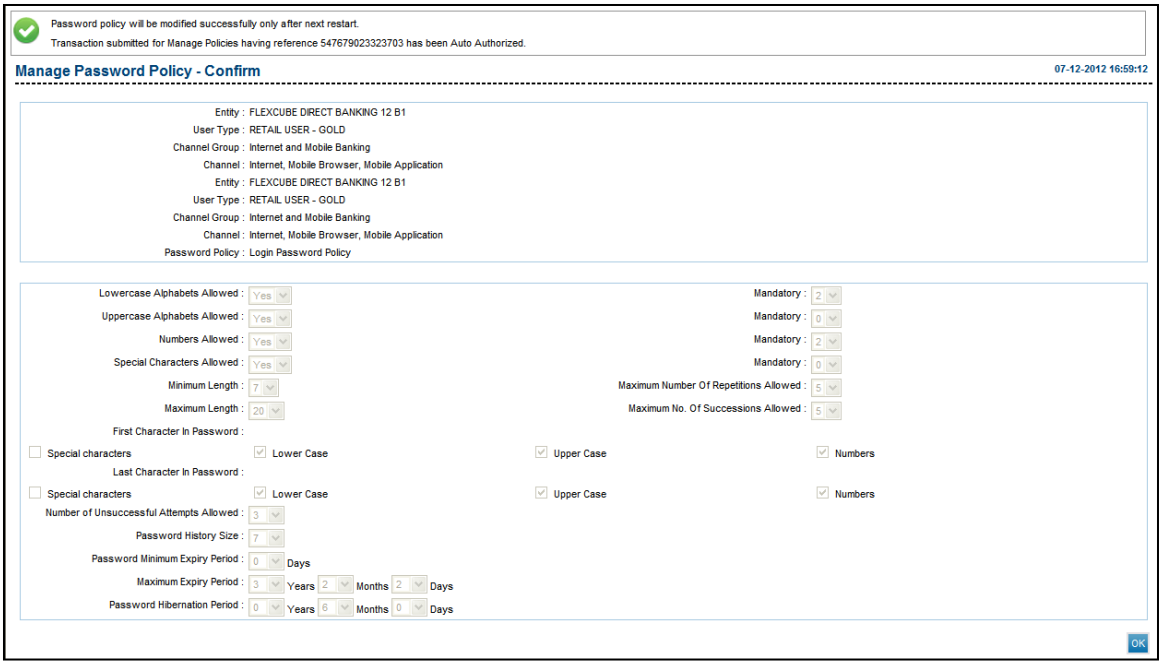
5. Click **Modify**.
The **Manage Password Policy - Verify** screen appears.
OR
Click **Back.**
The **Manage Policy – Login Password Policy** screen appears.

Manage Password Policy - Verify



6. Click **Confirm**.
The **Manage Password Policy - Confirm** screen with the status message appears.
OR
Click **Change**.
The **Manage Password Policy - Verify** screen appears.

Manage Password Policy - Confirm



7. Click **OK**.
The **Manage Policy** screen appears.

5.2 Automatic Unlock of Transaction Password

If a user enters the incorrect password consecutively for more than particular number of times, the *Transaction Password* is then locked. The system then unlocks the same after the specific time set during the configuration.

Note: Please refer to the following example for easier understanding of the feature.

For Example:

The *Transaction Password* is/can be locked in the following situation:

Scenario	Result
If a user enters the incorrect *Transaction Password* **5 times** *(Default OR value set by the user)* consecutively within the same day.	The *Transaction Password* remains *unlocked*.
If a user enters the incorrect *Transaction Password* **6 times** *(Default OR value set by the user)* consecutively within the same day.	The *Transaction Password* gets locked and is *automatically unlocked after **24** hours*.
If a user enters the incorrect transaction password **10 times** *(Default OR value set by the user)* consecutively within the same day.	The *Transaction Password* gets locked and is *automatically unlocked after **24** hours*.
If a user enters the incorrect transaction password **11 times** *(Default OR value set by the user)* consecutively within the same day.	The *Transaction Password* gets locked and will have to be *manually unlocked* by the *bank or corporate administrator*.

Note: The user is notified while locking the *Transaction Password*.